# Border Directory Concept

**January 6, 1999**

Prepared for:
Federal PKI - Technical Working Group

CYGNACOM SOLUTIONS

# 1 Introduction

## *1.1 Background*

The Federal PKI will be knit together from numerous agency PKIs, some initially limited to particular applications, and some agency-wide (or enterprise scale) multi-application PKIs. It will not be a monolithic, structure, nor will it be a single enterprise PKI. These will use CA products or services from different vendors, as well as client products from many vendors. The approach adopted for the Federal PKI is based on the concept of a “bridge CA,” that provides trust (or certification) paths between “principal CAs” in each agency. Industry organizations and other nations are adopting similar solutions, where a designated CA cross-certifies with high level CAs in different trust domains, to create certification paths. This approach will allow a large-scale government, industry, national or global PKI to be assembled from application or enterprise scale PKIs. The architecture is illustrated in Figure 1. The approach is further described in [TWG-98-29] and the Federal PKI Concept of Operations [CONOPS].

However, the very first step to verify a digital signature is to build a certificate path. For the bridge CA approach to work, Directory User Agents (DUA) must be able to retrieve certificates and certificate revocation information. The Border Directory concept described in this paper will provide a mechanism for all DUA's to build certificate paths to all parties within a Trust Domain that has cross-certified with the Bridge CA.

In addition, the directory needs to provide the Certificate Policies (CP) and Certificate Practice Statements (CPS) [CHOK] to the users of the Federal PKI.

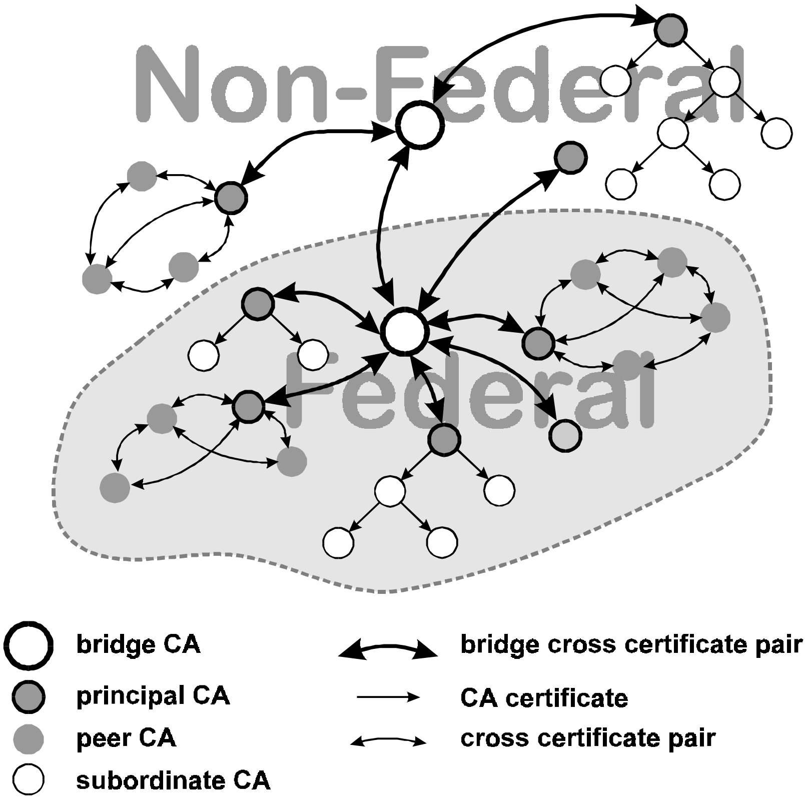

**Figure 1 - The FPKI Certification Path Architecture**

### 1.2 Scope

This document describes the Border Directory concept. The Border Directory is designed only to provide the following services:

- Certificate Path development
- Revocation Information Retrieval
- Certificate Policy and Certificate Practice Statement retrieval

The following section describes the architecture of the Border Directory concept.

## 2 Border Directory Architecture

The main purpose of the Border Directory is to provide a means for applications to build certificate paths during verification of a digital signature. The Border Directory model is outlined in the figure below:

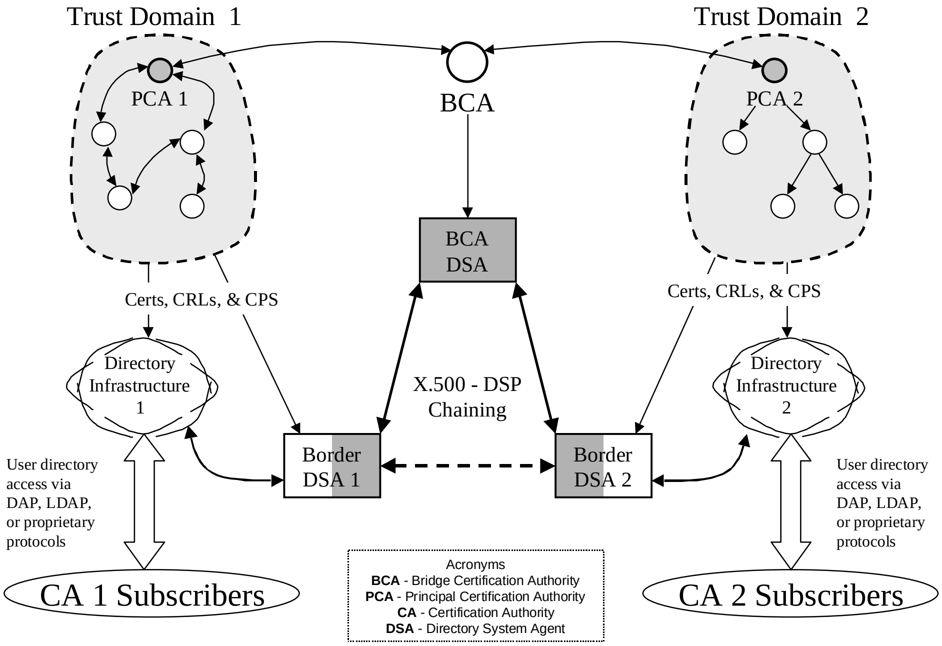
Trust Domain 1
Trust Domain 2
PCA 1
BCA
PCA 2
BCA DSA
Certs, CRLs, & CPS
Certs, CRLs, & CPS
Directory Infrastructure 1
X.500 - DSP Chaining
Directory Infrastructure 2
User directory access via DAP, LDAP, or proprietary protocols
Border DSA 1
Border DSA 2
User directory access via DAP, LDAP, or proprietary protocols
CA 1 Subscribers
CA 2 Subscribers
Acronyms
BCA - Bridge Certification Authority
PCA - Principal Certification Authority
CA - Certification Authority
DSA - Directory System Agent

**Figure 2 - Border Directory Architectural Concept**

For every Trust Domain that wishes to "cross-certify" with the Bridge CA, the Federal PKI will require that the Trust Domain maintain at a minimum of one Border Directory Service Agent (DSA). The mechanism that a Trust Domain chooses to post certificates and certificate revocation information may be through chaining, LDAP, referrals, or any type of proprietary mechanism. All Border DSA's will be maintained by the Trust Domain as defined in each PCA's Certificate Practice Statement. A Border DSA does not need to store the entire Directory Information Base. Border Directories are capable of obtaining information on behalf of a DUA in its trust domain. This information includes any certificate, CRL, or CPS outside a DUA's Trust Domain.

## 2.1 Border Directory Components

The following are descriptions of all entities involved with the Border Directory concept. The definitions and terms used are consistent with those defined in the Proposed Federal PKI Concept of Operation [Burr].

- **Federal Policy Management Authority (FPMA)**: This management authority sets the overall policies of the Federal PKI, and approves the policies and procedures of trust domains within the federal PKI. It operates the Federal Bridge CA and BCA DSA.
- **Trust Domain**: In the Federal context a trust domain is a portion of the Federal PKI that operates under the management of a single policy management authority. One or more CA's exist within the trust domain. Each trust domain has a single principal CA, but may have many other CAs. Each trust domain has a domain repository. In the non-Federal context, trust domains, may be more loosely organized, but consist at a minimum of a group of CAs that share trust and operate under consistent policies.
- **Directory Infrastructure**: One or more DSA's that provide directory services for a trust domain. The directories may include information that is proprietary within the organization. Directories may also be responsible for replicating the necessary certificate information to the Border Directory.
- **Bridge Certificate Authority (BCA)**: The Federal Bridge CA is operated by the Federal Policy Management Authority. Its purpose is to be a bridge of trust that provides trust paths between the various trust domains of the Federal PKI, as well as between the Federal PKI and non-federal trust domains. Trust domains that operate with policies and practices that are approved by the FPMA, designate a principal CA that is eligible to cross-certify with the Federal BCA. The BCA also issues a consolidated Federal CA CRL.
- **Principal Certification Authority (PCA)**: A CA within a trust domain that cross-certifies with the Federal BCA. Each trust domain has one principal CA. In the case of a domain with hierarchical certification paths, it will be the root CA of the domain. In a mesh-organized domain, the principal CA may be any CA in the domain. However, it will normally be one operated by, or associated with, the domain policy management authority.
- **BCA Directory Service Agent (BCA DSA)**: The BCA repository will be open to Internet access by anyone, and will make available:
  - All certificates issued by the BCA
  - All certificates held by the BCA
  - All cross certificate pairs containing certificates held or issued by the BCA
  - All CA certificates issued by CAs within the overall Federal PKI
  - All cross certificate pairs between CAs in the Federal PKI
  - CP and CPS's for all CA's within a Trust Domain that has cross-certified with the BCA.
  - A consolidated Federal CA (indirect) CRL that covers all CAs in the Federal PKI. This implies a requirement to include appropriate CRL Issuer and CRL Distribution Point extensions in all CA Certificates issued by CAs within the Federal PKI
  - Other certificates and CRLs as determined by the FPMA
- **Border DSA**: Provides the directory infrastructure backbone for the FPKI. These directories should contain all the certificates, revocation information, and CP and CPS's that the organization has deemed appropriate for posting. All Border DSA's will also contain a copy of the consolidated ARL.

## 2.2 Border Directory Requirements

Border Directories provides a mechanism for Directory User Agents (within the Federal PKI) to retrieve certificates and certificate revocation information without adding the complexity of multiple directory access protocols. Border Directories allow agencies to keep existing directory implementations as well as create new custom directory structures and still be able to communicate within the Federal PKI. In essence, each Border DSA has two sets of interfaces: one with the Bridge CA DSA and one with the Trust Domain that it serves.

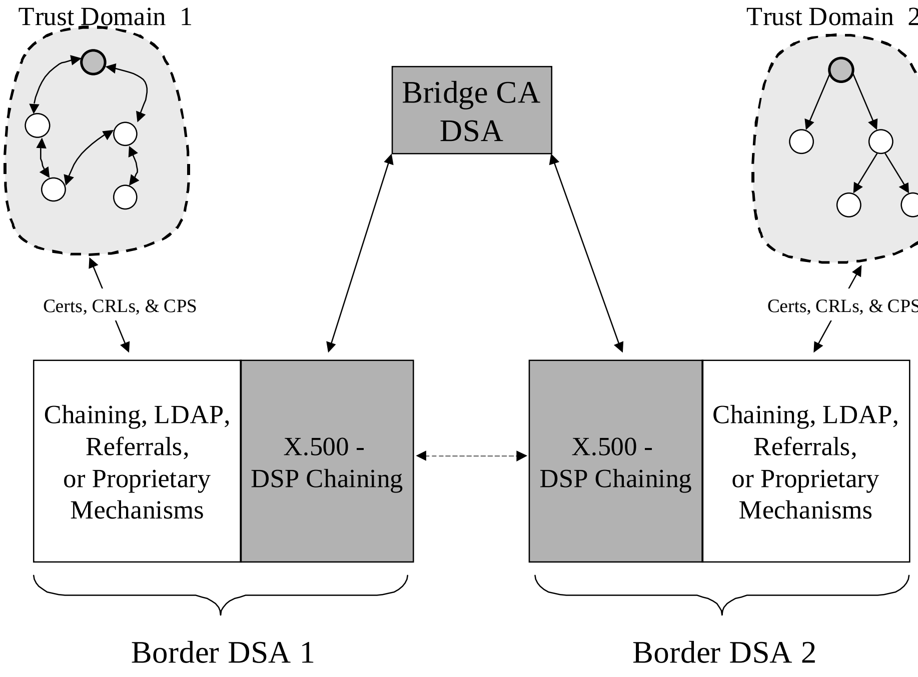

**Figure 3 - Border Directory Requirements**

### 2.2.1 Bridge CA Interface

All Border Directories must be able to support Directory Service Protocol (DSP) chaining as defined in the X.500 Directory Services Standard. The Border Directories will be able to query other Border Directories for the certificate or certificate revocation information on behalf of an application. In addition, the CA's within each Trust Domain must post certificates and revocation notification information to the Border Directories as defined in their Certificate Practice Statement.

All Border DSA's must be chained, at a minimum, to the BCA DSA. Border DSA's may chain with other Border DSA's in an effort to provide more efficient certificate path development.

Trust domains wishing to cross-certify with the Bridge CA will be required to meet these Border Directory requirements.

### 2.2.2 Trust Domain Interface

The Border Directory concept does not dictate any requirements for directories within a Trust Domain. Trust Domains are given the flexibility to provide the directory services best suited for their respective infrastructures.

### 2.3 Border Directory Features

The following are features of the Border Directory concept:

- Does not require Directory User Agents to be able to handle different directory access protocols (LDAP v2, LDAP v3, DAP, etc.)
- Requires that all Trust Domains develop at a minimum of one Border DSA
- Does not require changes to legacy applications
- Does not impact CA to Directory/Repository protocols or interactions
- Allows various agencies to implement local policies regarding who accesses which directory entries

# 3 References

[BURR] Proposed Federal Public Key Infrastructure Concept of Operations, 4 September, 1998

[CHOK] Certificate Policy and Certification Practices Framework, S. Chokhani and W. Ford, Informational RFC, IETF PKIX Part IV, July 1997.

[CONOPS] TWG-98-31, *Draft Federal PKI Concept of Operations*, 3 June 1998

[TWG-98-29] W. E. Burr, “Proposed Federal PKI Architecture,” 19 May 1998